Progress in Electric Utilities Risk Management – Emerging Guidance

Bill Jenkins
Coalfire
April 17, 2012

IEEE REPC
Rural Electric Power Conference

Authors

Bao Le, PE, CISM, IEEE member
Vice President, Corporate Development
Coalfire
361 Centennial Pkwy Suite 150
Louisville, CO 80027 USA
Bao.Le@coalfiresystsems.com

Bill Jenkins, CISSP, CISA, GPEN, FITSP-M
Senior Security Engineer
Coalfire
361 Centennial Pkwy, Suite 150
Louisville, CO 80027 USA
Bill.Jenkins@coalfiresystems.com

Agenda

I. Background

II. DOE Initiative

III. Elements

IV. Risk Cycle

V. Combined

VI. Projected Impacts

VII. Looking Ahead

VIII. Questions

Background

- Hot Topic
  - *Protection of Electric Utilities and other Critical Infrastructure Elements*
- Maturing Response
  - Mostly Reactive
  - Point Solutions
  - Push Back on Costs
  - Focus on Individual Threats and Assets
- Key Unanswered Question:

What is the overall Sector Risk?

Department of Energy Initiative

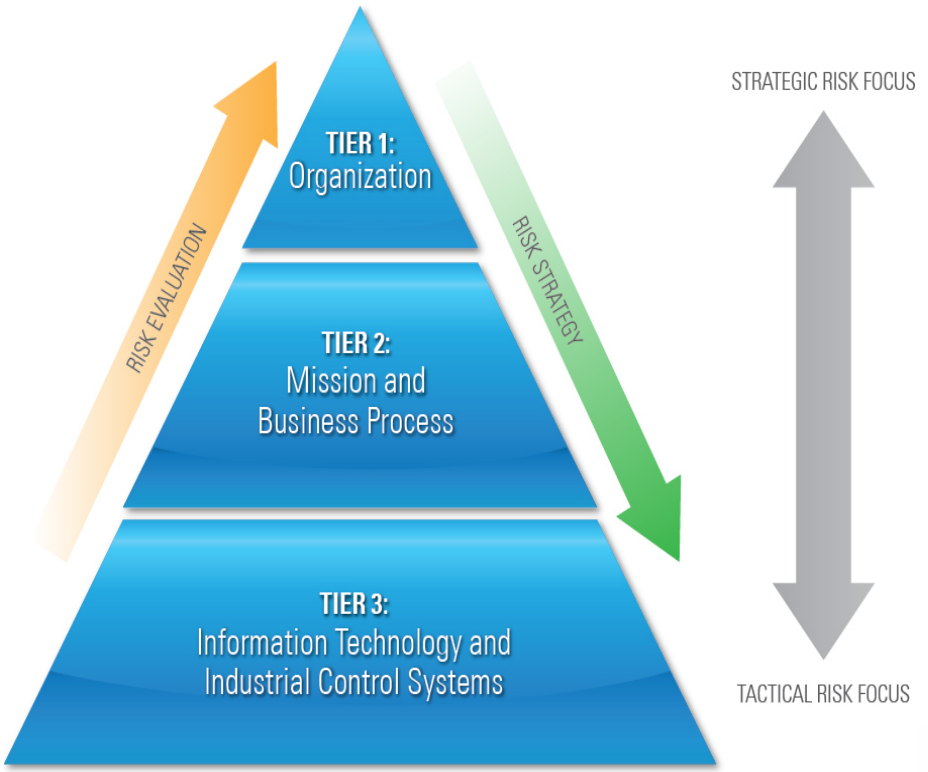
- NIST Special Publication 800-39
  - Managing Information Security Risk Organization, Mission, and Information System View
  - Issued March 2011
- DOE Tuned for Electric Sector
  - In collaboration with NIST, NERC, and other Community Stakeholders
- Result

Electricity Subsector Cybersecurity Risk Management Process

- A Guideline
  - "… not intended to replace or subsume other risk-related activities, programs, processes, or approaches that electricity subsector organizations have implemented."
  - "… not part of any regulatory framework."
  - "… complementary to, and should be used as part of, a more comprehensive enterprise risk management program."

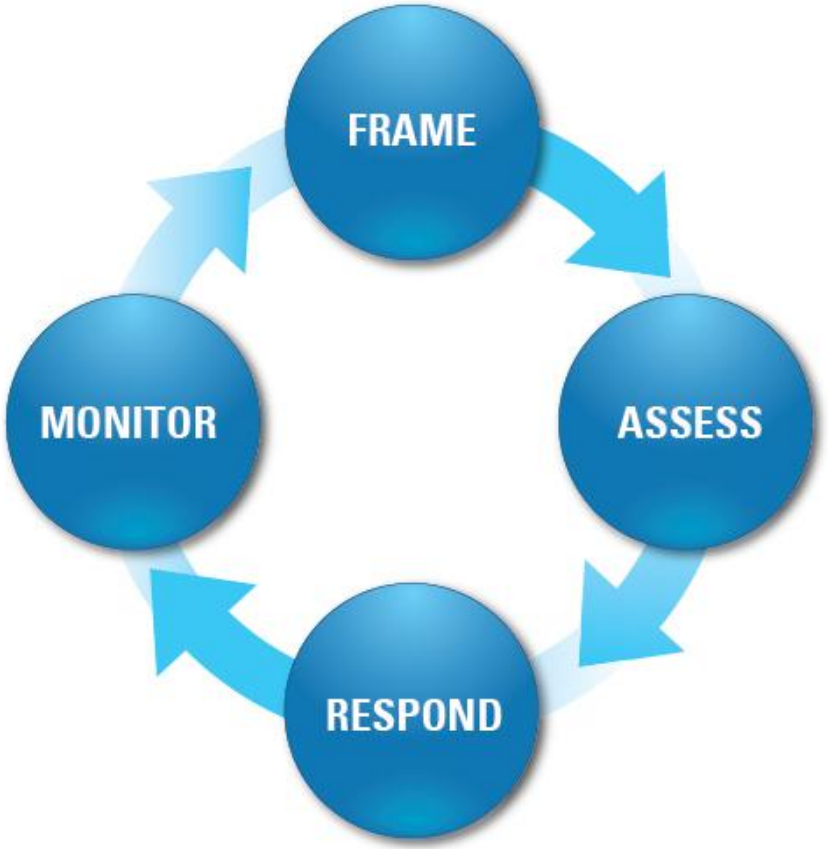
Tiered Model

- Organization
  - Board of Directors and C-level executives
  - Establish governance and reporting
  - Define risk tolerance
  - Establish business objectives and priorities for making trade-offs
  - Defining risk appetite
- Mission and Business Processes
  - Most of the organization's operations
  - Create and enforce required business processes
  - Provide for a disciplined and structured management and monitoring of IT and ICS assets
  - Integrate cyber requirements to processes and planning activities
  - Promote the cost-effective, efficient, and resilient systems
- Information Technology and Industrial Control Systems
  - Contains the specification, acquisition, operation, and monitoring of cyber security controls
  - Determination of IT and ICS asset value and risk
  - Identification and deployment of cyber controls
  - Routine environment assessment and monitoring
  - Response to changes in threats and vulnerabilities

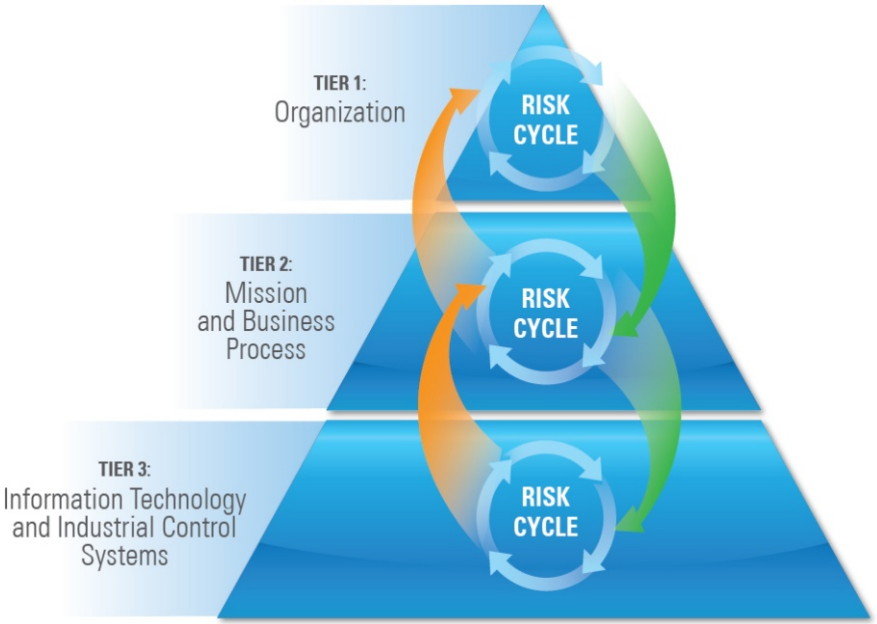


Risk Management Cycle

- Frame
  - Scope and Context
  - External Dependencies
  - Trust Relationships
- Assess
  - Identification and Evaluation of:
    - Threats
    - Vulnerabilities
    - Potential Impact
    - Likelihood of Occurrence
  - Risk => threat, vulnerability, likelihood, consequence/impact
- Respond
  - Determine Alternatives
  - Trade-offs
- Monitor
  - Verify Implementation
  - Determine effectiveness

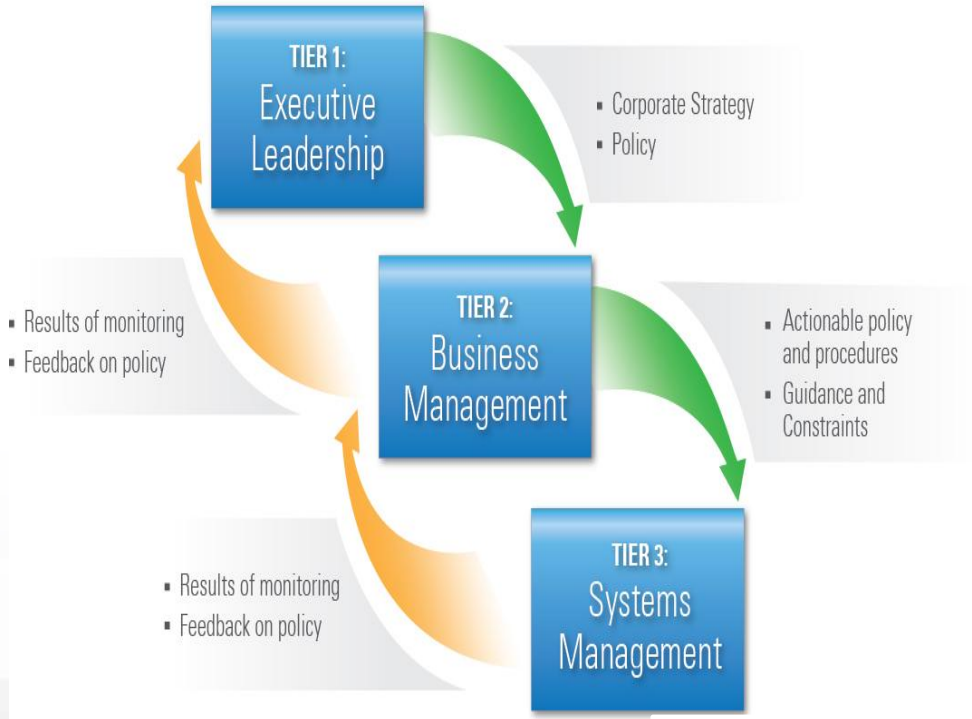


Putting it all Together



Each Tier Informs and Learns from the Others

Complements Existing Roles and Responsibilities



Risk Responses

- Acceptance
- Avoidance
- Sharing and Transfer
- Mitigation

Projected Impacts

- Documentation and Processes
  - A suggested minimum floor of analysis, process, and documentation
  - Can augment existing management activities
- Liability
  - Cyber-based outages are coming
  - Impacted parties will seek recourse
  - Participation in a recognized risk management process
    - Provides a solid basis for defending decisions
- Enabling Sector Visibility and Insight
  - Establishes a common vocabulary
  - Data and experiences can be shared – lessons learned
  - Framework for identifying national remediation initiatives

Looking Ahead

- Most Current Version March 2012
  - http://energy.gov/sites/prod/files/RMP%20Guideline%20Second%20Draft%20for%20Public%20Comment%20-%20March%202012.pdf
  - Public Comments Closed 5 April
  - Expect Finalization in 45-60 Days
- Difficult to Ignore
  - Based on widely accepted principles
  - NIST Foundation
  - Supported by Key Stakeholders – NIST, DOE, NERC, others
- Next Steps
  - Review Current Version
  - Conduct Preliminary Gap Analysis with Current Practices
  - Seek Opportunities for Gradual Adoption

Questions

Goalfire℠